PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-347949

(43)Date of publication of application : 03.12.1992

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00
H04L 12/54
H04L 12/58

(21)Application number : 03-158023

(22)Date of filing : 28.06.1991

(71)Applicant : TOSHIBA CORP

(72)Inventor : KAWAMURA SHINICHI
SHINPO ATSUSHI

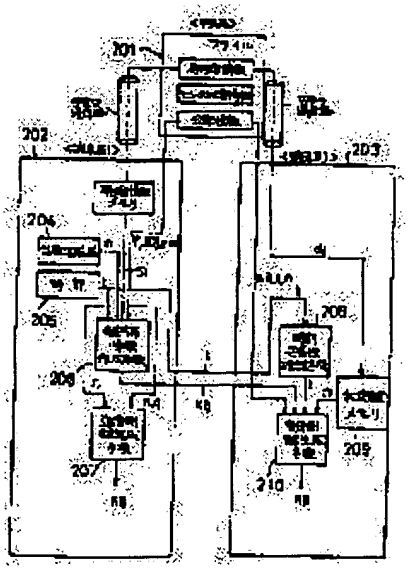
(30)Priority

Priority number : 02305972 Priority date : 14.11.1990 Priority country : JP

(54) CIPHER COMMUNICATING METHOD AND CIPHER COMMUNICATING SYSTEM

(57)Abstract:

PURPOSE: To make it possible to cope with the transfer of the electronic mail without complicating a communication system by decoding a ciphered simple sentence by the terminal station itself on a transmission side based on the key sharing information for unknown destinations even when a receiver of electronic mail is not present on a destination.



CONSTITUTION: A terminal station (i) transmitting ciphers generates the key of the transmission side based on not only the open information prepared by a central station 201, the station secret information but also the random number information Yi generated by the terminal station (i) on the transmission side and generates the key sharing information Xiy by further adding time information t. A terminal station (j) on the reception side confirms at first the validity of the reception time information (t), regards the information as a normal cipher and generates the key on the reception side based on the open information prepared by the central station 201, the station secret information, the received key sharing information Xij and the time information t. Next, whether the generated key of the reception side and the key generated at the terminal station (i) on the transmission side coincide or not is certified based on the

ciphering communication. When [redacted] coincide, the sharing of the key is for[redacted].

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平4－347949

(43)公開日　平成４年(1992)12月３日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｌ	9/06						
	9/14						
Ｇ０９Ｃ	1/00		7922－5L				
			7117－5K	Ｈ０４Ｌ	9／02	Ｚ	
			8529－5K		11／20	１０１　Ｂ	

審査請求　未請求　請求項の数５(全 14 頁)　最終頁に続く

(21)出願番号　特願平3－158023

(22)出願日　平成３年(1991)６月28日

(31)優先権主張番号　特願平2－305972

(32)優先日　平２(1990)11月14日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内

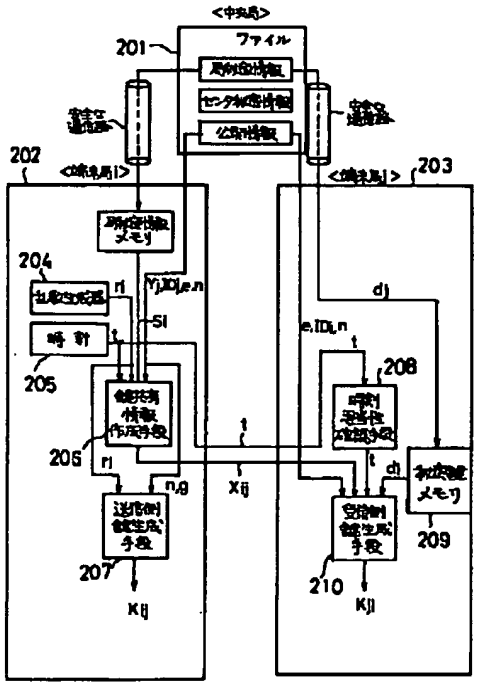
(74)代理人　弁理士　則近　憲佑

(54)【発明の名称】　暗号通信方法及び暗号通信システム

(57)【要約】

【構成】宛先不明用鍵共有情報に基づいて送信側端末局自身が暗号化された平文を復号する送信側復号手段を有する。

【効果】電子メールの送受信に於いて宛先に電子メールの受信者が存在しない場合でも通信システムを複雑にすること無く対処することが可能である。



1

【特許請求の範囲】

【請求項1】　中央局から複数の端末局のそれぞれに鍵を発行し、前記端末局の二局間で通信ネットワークを介して暗号通信する暗号通信方法において、前記中央局が全ての端末局に公開する同一の公開情報及び各端末局のそれぞれに知らせる相異なる局秘密情報を作成する工程と、前記中央局が前記公開情報及び前記局秘密情報を暗号送信側の端末局及び暗号受信側の端末局に発行する工程と、前記送信側端末局内で乱数情報を生成する工程と、前記送信側端末局内で時刻情報を出力する工程と、前記乱数情報及び前記公開情報に基づき送信側の鍵を生成する工程と、前記乱数情報、前記時刻情報、前記公開情報及び前記局秘密情報に基づき鍵共有情報を作成する工程と、前記時刻情報及び前記鍵共有情報を受信する端末局内で前記時刻情報が虚偽であるか否かを確認する工程と、前記受信側端末局内で前記時刻情報が虚偽でないと確認された時、前記時刻情報、並びに前記鍵共有情報、前記公開情報及び前記局秘密情報に基づき受信側の鍵を生成する工程と、前記送信側端末局内で生成された鍵と前記受信側端末局内で生成された鍵とが一致することを認証する工程とを備えたことを特徴とする暗号通信方法。

【請求項2】　中央局から通信ネットワークを介して複数の端末局のそれぞれに鍵を発行し、前記端末局の二局間で暗号通信する暗号通信システムにおいて、前記中央局が全ての端末局に公開する同一の公開情報及び各端末局のそれぞれに知らせる相異なる局秘密情報を作成する局秘密情報作成手段と、前記中央局が前記公開情報及び前記局秘密情報を暗号送信側の端末局及び暗号受信側の端末局に発行する情報発行手段と、前記送信側端末局内で乱数情報を生成する乱数情報生成手段と、前記送信側端末局内で時刻情報を出力する時刻情報出力手段と、前記乱数情報及び前記公開情報に基づき送信側の鍵を生成する送信側鍵生成手段と、前記乱数情報、前記時刻情報、前記公開情報及び前記局秘密情報に基づき鍵共有情報を作成する鍵共有情報作成手段と、前記時刻情報及び前記鍵共有情報を受信する端末局内で前記時刻情報が虚偽であるか否かを確認する時刻妥当性確認手段と、前記受信側端末局内で前記時刻情報が虚偽でないと認識された場合、前記時刻情報、並びに前記鍵共有情報、前記公開情報及び前記局秘密情報に基づき受信側の鍵を生成する受信側鍵生成手段と、前記送信側端末局内で生成された鍵と前記受信側端末局内で生成された鍵とが一致することを認証する認証手段とを備えたことを特徴とする暗号通信システム。

【請求項3】　中央局から複数の端末局のそれぞれに対し、端末局固有の秘密鍵を発行し、二局以上の前記端末局の間で通信ネットワークを介して暗号通信する暗号通信システムにおいて、前記端末局固有の秘密鍵は、封止されて成り、前記暗号通信の工程は変更不可能であることを特徴とする請求項(2) 記載の暗号通信システム。

2

【請求項4】　鍵共有情報作成手段で作成される鍵共有情報には送信側端末局自身で前記暗号化された平文を復号する宛先不明用鍵共有情報が含まれ、送信側鍵生成手段で生成された送信側の鍵を用いて平文を暗号化する平文暗号化手段と、該手段で暗号化された前記平文、並びに前記鍵共有情報作成手段で作成される鍵共有情報及び時刻情報出力手段で出力された時刻情報から送信電文を作成する送信電文作成手段と、該手段で作成された電文を受信側端末局で受信し電文内容を分割する電文内容分割手段と、該手段で分割された前記暗号化された平文を受信側鍵生成手段で生成された受信側の鍵を用いて復号する復号手段とを備え、更に受信側端末局の宛先が不明の場合、前記宛先不明用鍵共有情報に基づいて送信側端末局自身が前記暗号化された平文を復号する送信側復号手段を有することを特徴とする請求項(2) 記載の暗号通信システム。

【請求項5】　鍵共有情報作成手段で作成される鍵共有情報には送信側端末局自身で前記暗号化された平文を復号する鍵復元情報が含まれ、送信側鍵生成手段で生成された送信側の鍵を用いて平文を暗号化する平文暗号化手段と、該手段で暗号化された前記平文、並びに前記鍵共有情報を作成する手段で作成される鍵共有情報及び時刻情報を出力する手段で出力された時刻情報から送信電文を作成する送信電文作成手段と、該手段で作成された電文をファイルに格納する格納手段と、該手段で格納された前記暗号化された平文を前記鍵復元情報に基づいて送信側端末局自身が復号する送信側復号手段とを有することを特徴とする請求項(2) 記載の暗号通信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は暗号通信方法及び暗号通信システムに係わり、特に端末局間で共有する鍵の変更が容易であり、3局間以上の鍵共有も容易であり、かつ成り済ましによる再送攻撃を有効に防止することが可能である暗号通信方法及び暗号通信システムに関する。

【0002】

【従来の技術】従来から、第3者による盗聴又はメッセージの改ざんが起こり得るような安全でない通信路を介してデータの授受を行う場合、暗号を利用してそのデータを保護する様々な方式が研究され、かつ利用されている。

【0003】上記暗号方式は分類上、秘密鍵暗号（あるいは慣用暗号）と公開鍵暗号とに分けられる。秘密鍵暗号は、暗号化に使用する鍵とその復号化に使用する鍵が同じ暗号方式であり高速処理が容易であるので、広く利用されている。但しこの秘密鍵暗号の場合には、暗号通信に先立って送信者と受信者との間で同一の鍵情報を第3者に知られないように安全に共有しておかなければならない。すなわち鍵共有が必要である。原始的な鍵共有

方法として通信相手の所まで人が出向き、次いで使用する鍵を事前に打ち合わせる方法がある。軍事、外交用ではこのような手間の掛かる方法で鍵共有することも許容できるが、商用通信には不向きである。一方、公開鍵暗号は、暗号化の鍵とその復号化の鍵が異なり、暗号化の鍵は公開情報であり誰もが知ることができ、復号鍵のみを各自が秘密に保持する方式である。この方式では暗号化の鍵が公開されているので鍵共有は必要なく、公開されている鍵を用いて所望の相手と暗号通信が可能である。公開鍵の管理方法の一例として、公開鍵をユーザ毎にリスト化して誰もが参照可能なデータベースに登録する方法がある。この場合、公開鍵暗号を正しく運用するため公開鍵のリストに登録されている鍵が改ざんされていないことを保証しなければならない。すなわち公開鍵の認証機能が必要である。

【０００４】しかしながら、公開鍵暗号は鍵の管理が簡便であるという長所がある反面、処理速度が比較的低いという欠点がある。そこで、公開鍵暗号の技術を利用して送信者と受信者との間で同一の鍵情報を共有しておき、その後にその鍵情報を用いて秘密鍵暗号で暗号通信を行うという幾つかの方式が実行されている。これらの方式で最初に提案されたものとしてＤＨ方式（W.Diffie &M.E.Hellman, "NewDirections in cryptography" IEEE Trans. on Information Theory, IT-22,6,pp.644-645 (June 1976)）が知られている。ＤＨ方式は、大きい素数ｐを法とするべき乗演算の逆変換が困難であることに基づいた二者間に限定した鍵配送方式である。つまり数学上、

$y = g^x \mod p$　　（x、gは整数）

において、g^x をｐで割った余りの値ｙをｘから求めることは簡単であるが、値ｙから値ｘを求めることは困難であることに基づく。この方式では公開鍵の認証機能がなく、かつ送受信者間で共有される鍵は変化することがなかった。その後、共有される鍵が毎回変わるように改良を加え、かつ３者以上の間で鍵を共有できるようにした幾つかの方式が提案されている。

【０００５】改良方式の一つとして岡本龍明氏等による改良は二者以上の鍵共有への拡張と位置付けられる（岡本、白石“ＰＫＤＳに基づく共有鍵配送方式”昭和５９年度電子通信学会通信部門全国大会講演論文集 No.18）。

【０００６】しかしながら、上記改良方式は素数ｐを法とするべき乗演算を用いているので、公開鍵のリストは第３者による改ざんがないという仮定が必要であった。又は、第３者による改ざんを防ぐための仕組み、例えば認証機能を別個に設ける必要があった。

【０００７】それで、岡本栄司氏は法を二つの素数ｐ，ｑの積に拡張することによって公開情報を認証する機構を鍵共有法に組み込んだ方式を提案した("Proposal for identity-based key distribution systems", Electronics Letters, Vol.22,No.24,pp.1283-1284, 1986）。しかしながら、この方式では共有した鍵が送信局ｉと受信局ｊの両方の秘密情報に依存しており、３者以上の鍵共有には向かない。

【０００８】小山－太田方式（Security of improvedid entity-based conference keydistribution systems", Lecture Notes in Computer Science Advances incrypt ology -Eurocrypt'88- pp.11-19, Springer-Verlag 1988）は上記二人の岡本氏の方式の長所をそれぞれ取り込み、かつ法を３つの素数の積としたものである。しかしながら、この方式では二つの素数の積を法とする方式に比べ法の桁数が約２倍になってしまい、メモリ量及び演算量の観点から不利である。例えばべき乗計算の演算量は概ね法の桁数の３乗に比例するので、１回のべき乗計算につき演算量は約８倍に達する。

【０００９】また伊藤等は、毎回鍵が変わり、かつグループ鍵共有が可能であり、小山－太田方式よりも演算量の少ない方式を提案している（伊藤、羽物、笹瀬、森：“ＩＤ情報に基づく公開ファイル不要な一方向鍵配送方式”、1990年電子情報通信学会春季全国大会講演論文集、No.A-283, p.1-283, 1990, 3月）。しかしながら、伊藤等の方式をグループ鍵共有に用いた場合、グループ内の第３者の再送攻撃による成り済ましや、送信者秘密情報などの問題点が存在する。

【００１０】上記の如く、鍵配送方式の改良に対する技術の進展と同時に、短文のデータのみならず上記鍵配送方式を用いて長文を伝送する試みが行われている。例えば、上記伊藤等のグループ鍵共有を利用した鍵配送方式に基づき、電子メールをユーザへ送信することが行われている。

【００１１】電子メールの具体例としてＵＮＩＸネットワークのメールがある。このメール・システムは複数のＵＮＩＸマシンを通信回路でメッシュ状に接続したネットワーク上を送信端末から受信端末へバケツ・リレー的にメッセージを送り付けるものであり、現在広く使われている。このような電子メールでは同一のメッセージを複数の宛先に送り付ける同報通信機能が一般にサポートされている。また、メールに不可欠な機能として宛先アドレスの誤り、及び相手のアドレスが変更されていて送信者が指定した相手にメールを配達できなかった場合に、メールを送信元まで返送し、その旨送信者に通知する機能がある。ＵＮＩＸメールにおいてもこれらの機能がサポートされている。

【００１２】このようにメールにおいて重要なメッセージをやり取りする場合には、その内容を保護するためにメッセージを暗号化することが望ましい。また、その暗号通信は同報通信機能及び宛先不明メールの返信機能に対応している必要がある。上記機能を有する電子メールの従来例を図17に示す。

【００１３】図示するように、電子メールは送信者側の

5

アドレスID₁、受信者側のアドレスID₂、ID₃、…、鍵共有情報X₁₂、X₁₃、…、及び暗号文C＝E（K，M）から構成される。

【0014】上記従来例では、一送信者が同時に多数の受信者へ暗号化された電子メールを受信者毎に異なる暗号で伝送することができる。また、各受信者はその暗号化された電子メールを各受信者毎に異なる復号鍵を用いて復号することができる。

【0015】しかしながら、暗号メールを送信したときにそのメールが宛先不明で送信元に返送されてきた場合、送信者の当然の要求としてその暗号を復号して内容を確認したくなる。仮に送信者が自分のところに戻ってきた暗号メールを復号できないとすると送信者は宛先名のみから戻ってきたメールが自分が送信したメールのうちいずれであるかを判断しなければならない。

【0016】従って、万一宛先に電子メールの受信者が存在しない場合には、受信者は電子メールを復号することができない。換言すれば、返信された電子メールを復号するためには復号鍵を何等かの方法で受信者が記憶しておかなければならない。このように全ての送信された電子メールに対し復号鍵を記憶して管理することは通信システムを複雑化することになる。

【0017】

【発明が解決しようとする課題】上記の如く、鍵配送方式を用いたDH方式では2者間のみの通信であり、認証機能がなく、かつ公開鍵は変化しないので、第3者による盗聴又はメッセージの改ざんが高い確率で起こり得るという問題があった。

【0018】岡本龍明氏等による拡張された鍵共有方式では、3者以上で通信が可能であるけれども第3者によるメッセージの改ざんが高いという問題が依然として残っていた。

【0019】岡本栄司氏による二つの素数を用いた方式では、認証機能が取り込まれたため第3者による盗聴又はメッセージの改ざんの恐れが減少されたものの、3者以上の鍵共有には向かないという問題があった。

【0020】小山－太田方式では3者以上で通信が可能で、かつ認証機能が取り込まれているものの、演算量が大幅に増加するため実用化に適さないという問題があった。伊藤等の方式では、3者以上で通信が可能で認証機能が取り込まれ、かつ演算量もそれ程増加しないものの、グループ鍵共有に用いた場合に再送攻撃や秘密情報の漏洩等の問題点が存在した。

【0021】一方、暗号化された電子メールの送受信において、宛先に電子メールの受信者が存在しない事態に対し対処しようとした場合、通信システムが複雑になるという問題があった。

【0022】そこで、本発明は上記従来技術の問題点を解消するもので、その第1の目的とするところは、共有する鍵の変更が容易であり、3者以上の間での鍵共有も

6

可能であり、かつ成り済ましによる再送攻撃を有効に防止することが可能である暗号通信方法を提供することである。

【0023】第2の目的は、電子メールの送受信において宛先に電子メールの受信者が存在しない場合でも通信システムを複雑にすることなく対処可能である暗号通信方法を提供することである。また、上記暗号通信方法を実施するに有用である暗号通信システムを提供することである。

【0024】

【課題を解決するための手段】上記課題を解決するための本発明の暗号通信方法は、中央局から複数の端末局のそれぞれに鍵を発行し、2局の前記端末局間で通信ネットワークを介して暗号通信する暗号通信方法において、前記中央局が全ての端末局に公開する同一の公開情報及び各端末局のそれぞれに知らせる相異なる局秘密情報を作成する工程と、前記中央局が前記公開情報及び前記局秘密情報を暗号送信側の端末局及び暗号受信側の端末局に発行する工程と、前記送信側端末局内で乱数情報を生成する工程と、前記送信側端末局内で時刻情報を出力する工程と、前記乱数情報及び前記公開情報に基づき送信側の鍵を生成する工程と、前記乱数情報、前記時刻情報、前記公開情報及び前記局秘密情報に基づき鍵共有情報を作成する工程と、前記時刻情報及び前記鍵共有情報を受信する端末局内で前記時刻情報が虚偽であるか否かを確認する工程と、前記受信側端末局内で前記時刻情報が虚偽でないと確認された場合、前記時刻情報、並びに前記鍵共有情報、前記公開情報及び前記局秘密情報に基づき受信側の鍵を生成する工程と、前記受信側端末局内で生成された鍵と前記受信側端末局内で生成された鍵とが一致することを両者の比較により確認し、かつ一致することを認証する工程とを備えたことを特徴とする。

【0025】一方、本発明の暗号通信システムは、中央局から通信ネットワークを介して複数の端末局のそれぞれに鍵を発行し、2つの前記端末局間で暗号通信する暗号通信システムにおいて、前記中央局が全ての端末局に公開する同一の公開情報及び各端末局のそれぞれに知らせる相異なる局秘密情報を作成する局秘密情報作成手段と、前記中央局が前記公開情報及び前記局秘密情報を暗号送信側の端末局及び暗号受信側の端末局に発行する情報発行手段と、前記送信側端末局内で乱数情報を生成する乱数情報生成手段と、前記送信側端末局内で時刻情報を出力する時刻情報手段と、前記乱数情報及び前記公開情報に基づき送信側の鍵を生成する送信側鍵生成手段と、前記乱数情報、前記時刻情報、前記公開情報及び前記局秘密情報に基づき鍵共有情報を作成する鍵共有情報作成手段と、前記時刻情報及び前記鍵共有情報を受信する端末局内で前記時刻情報が虚偽であるか否かを確認する時刻妥当性確認手段と、前記受信側端末局内で前記時刻情報が虚偽でないと確認された場合、前記時刻情報、

並びに前記鍵共有情報、前記公開情報及び前記局秘密情報に基づき受信側の鍵を生成する受信側鍵生成手段と、前記送信側端末局内で生成された鍵と前記受信側端末局内で生成された鍵とが一致することを認証する認証手段とを備えたことを特徴とする

【００２６】さらに本発明による、前記端末局の二局以上のグループ鍵共有・同報暗号通信を行う暗号通信システムでは、前記局秘密情報を当該局の利用者に対しても秘密に保ち、また、前記局秘密情報を前記グループ鍵共有の工程以外では、使用不可能であるように装置構成することにより、グループ鍵共有の場面で問題となる秘密情報の漏洩を防止することを特徴とする。

【００２７】選択次第では、鍵共有情報作成手段で作成される鍵共有情報には送信側端末局自身で前記暗号化された平文を復号する宛先不明用鍵共有情報が含まれ、送信側鍵生成手段で生成された送信側の鍵を用いて平文を暗号化する平文暗号化手段と、該手段で暗号化された前記平文、並びに前記鍵共有情報作成手段で作成される鍵共有情報及び時刻情報出力手段で出力された時刻情報から送信電文を作成する送信電文作成手段と、該手段で作成された電文を受信側端末局で受信し電文内容を分割する電文内容分割手段と、該手段で分割された前記暗号化された平文を受信側鍵生成手段で生成された受信側の鍵を用いて復号する復号手段とを備え、更に受信側端末局の宛先が不明の場合、前記宛先不明用鍵共有情報に基づいて送信側端末局自身が前記暗号化された平文を復号する送信側復号手段を有することを特徴としても良い。

【００２８】

【作用】本発明の暗号通信方法では、暗号を送信する端末局は、中央局で作成される公開情報及び局秘密情報のみならず、送信側端末局自体が生成する乱数情報に基づいて送信側の鍵を生成し、かつ時刻情報を更に加えて鍵共有情報を生成する。この鍵共有情報及び時刻情報は暗号を受信する端末局に送信され受信側の鍵が生成される。すなわち、受信側端末局は、まず最初に受信した時刻情報の妥当性を確認する。妥当性が確認されると正規の暗号であると見なし、中央局で作成される公開情報及び局秘密情報、並びに受信した鍵共有情報及び時刻情報に基づき受信側の鍵を生成する。

【００２９】次いで、生成された受信側の鍵が送信側端末局で生成された鍵と一致するか否かの認証が暗号通信に基づいて行われ、一致する場合には鍵の共有が成立する。つまり、正しい暗号が送られたものとして受信側端末局は暗号情報を受け取る。従って、送信側端末局が乱数情報を自ら生成するので、暗号通信の度に簡単に鍵共有情報及び共有することになる鍵を変えることができる。共有される鍵の値は、送信者の生成する乱数情報のみに依存するので、原理的には、同じ乱数を用いて多数の受信側端末局に共通の鍵を配送することが可能である。しかし、このような使用法では、複数の受信端末局が結託し、それら局の秘密情報を受信者からの鍵配送情報に作用させると送信局の秘密情報が漏洩する可能性が存在する。そこで、このようなグループ鍵共有における不正操作を防止し、送信局秘密情報の漏洩を防止する目的で、本発明では、各局の秘密情報は当該局が自由に使用できる情報ではなく、当該局であってもその値を知らず、また、正当な鍵共有手順以外には使用できないように装置構成することを特徴としている。このようにすることにより、グループ鍵共有への適用が可能となる。

【００３０】さらに、鍵共有のために通信ネットワークに通す鍵共有情報は時刻に依存しているので、ある時刻に作成した鍵共有情報を後に再び利用することは困難である。そのため、３者以上のグループ鍵共有においても成り済ましによるメッセージの再送攻撃が困難になる。また、本発明では１つの素数を法とするのではなく２つの素数の積を法としているため、端末局認証用の局秘密情報を用いて認証機能を実現することが容易である。なお、本発明では３つ以上の素数の積を法とする方式に比べてメモリ、計算量の節約となる。

【００３１】選択次第では、鍵共有情報に宛先不明用鍵共有情報を含ませ、受信側端末局に送信される暗号化された平文に上記鍵共有情報を載せても良い。すなわち、受信側端末局が存在しない場合に送信側端末局に暗号化された平文を返信し、送信側端末局自身が上記宛先不明用鍵共有情報を用いて暗号化された平文を復号する。このようにすることにより、送信側端末局は受信側端末局が存在しない場合でも平文の内容を知ることができ管理上便利である。

【００３２】

【実施例】以下本発明の実施例を図面を参照して説明する。図１に本発明の第１実施例に係わる暗号通信システムのブロック図を示す。

【００３３】図示すように、暗号通信システムは該システムを立ち上げる中央局２０１と、該中央局２０１に通信ネットワークを介して接続される端末局ｉ，ｊ，…とを備える。但し、図１においては便宜上、端末局ｉ，ｊのみが示される。

【００３４】中央局２０１はプログラムにより予め定められた手順に従って、公開情報、中央局秘密情報、及び局秘密情報を算出すると共に、これらの情報をメモリする。ここで、公開情報とは全ての端末局ｉ，ｊ，…が中央局２０１との通信により自由に知ることができる情報であり、暗号通信システムの共通の法ｎ、プログラム内で予め定められる所定の整数ｇ，中央局の公開鍵ｅ，疑似ランダム関数h_1（ ）及びh_2（ ）端末局ｉ，ｊ，…の公開情報Ｙｉ，Ｙｊ，…、並びに端末局ｉ，ｊ，…の一意に定まる名前を数値化したＩＤｉ，ＩＤｊ，…から成る。

【００３５】これら公開情報は公開情報ゆえに管理運用法の自由度も大きい。図１では中央局の公開情報ファイ

ルから読み出す方法が示されている。実際には中央局の公開鍵e、法n、整数gは通信相手によらず一定だから各端末局はシステム加入時に一度だけ公開鍵e、法n、整数gを入手し、記録しておくだけで良い。また名前ID1，IDj，…及び公開情報Y1，Yj，…は中央局から入手する以外に、通信相手から入手しても良い。

【0036】中央局秘密情報とは中央局201が各端末局に対し秘密に保つ情報であり、相異なる2つの大きい素数p及びq、中央局内の法L、中央局固有の秘密鍵d、及び端末局1，j，…に対する中央局の秘密鍵e_1，e_1，…から成る。

【0037】局秘密情報とは中央局201と特定の端末局以外の局に対し秘密に保たれる情報であり、特定の端末局が1である場合、端末局1の秘密鍵d_1、及び端末局1認証用の秘密情報S1から成る。なお、中央局201は秘密鍵d_1，d_j，…、秘密情報S1，Sjを各端末局1，j，…に発行した後は局秘密情報を記録しておく必要はない。これら局秘密情報は完全かつ確実に対応する端末局に渡される。具体的方法として、例えば局秘密情報は安全に持ち運び可能なICカードのような記憶媒体に保管して各局に渡す方法がある。図1では、中央局が各端末局に安全に局秘密情報を発行する手続を「安全な通信路」として示している。上記の各情報の生成方法は後述する。

【0038】端末局1，j，…のそれぞれは暗号情報の送信部202及び受信部203を備える。例えば暗号情報が端末局1の送信部202から端末局jの受信部203へ送信される場合、乱数情報r_1を生成する乱数生成器204と、時刻情報tを出力する時計205と、中央局201から入手した各種公開情報及び局秘密情報、並びに乱数情報r1及び時刻情報tを用いて鍵共有情報X_{1j}を作成する鍵共有情報作成手段206と、公開情報g及び乱数情報r_1を用いて端末局1の共有鍵K_{1j}を生成する送信側鍵生成手段207とを備える。

【0039】また、端末局jの受信部203は端末局1から入手する時刻情報tが虚偽であるか否かを確認する時刻妥当性確認手段208と、中央局201から秘密鍵d_1を入手し保持する秘密鍵メモリ209と、中央局201から入手した各種公開情報、虚偽でないと確認された時刻情報t、秘密鍵d_1及び端末局1の鍵共有情報作成手段206から出力される鍵共有情報X_{1j}を用いて端末局jの共有鍵K_{1j}を生成する受信側鍵生成手段210とを備える。以上の構成において、まず最初に中央局201内で行われる各種情報の作成方法を説明する。

【0040】中央局201は最初に相異なる二つの大きい素数p、qを適宜生成し、その積n＝p・qを作成する。また、p－1とq－1の最小公倍数であるLを定める。次にガロア体（ガロアフィールド）GF（p）とGF（q）の両方で生成元となる整数gを一つ選定する。この条件は本発明の第1実施例に係わる暗号通信システムの安全性を向上させるために導入されている。但し、$1<g\leqq n-1$の範囲の任意の整数値gを用いても構わない。また、中央局201の公開鍵eをLと互いに素である整数群から一つ選定し、次いで公開鍵eに対応する中央局201の秘密鍵dを、

$$e\cdot d=1 \pmod L$$

を満たすように作成する。ここで、上式はeとdとの積として定まる値に1を差し引いた値がLで割り切れることを示す。さらに、公開の共通の底Gを、

$$G=g^f \bmod n$$

を満たすように定める。ここで、$f=d^k$であり、Gはg^fの値をnで割ったときの余りの値を意味する。kは鍵共有のプロセスによって定まる非負整数（零及び自然数）である。

【0041】次に、中央局201は端末局1の秘密鍵d_1を秘密鍵dの値と異なり、かつLと互いに素である整数群から一つ選定する。ここで、各端末局1，j，…に対する秘密鍵d_1、d_j、…は互いに異なるように選定される。次いで、d_1に対し、

$$e_1\cdot d_1-1 \pmod L$$

の関係を満たす中央局の秘密鍵e_1が定められる。また、中央局201は上記の秘密鍵dの値を用いて局認証用の秘密情報S1を、

$$S1=h_1(ID1)^{-d} \bmod n$$

に従って定める。ここで、h_1（）は疑似ランダム関数である。最後に法nの下で、上記の底G、秘密鍵e_1、秘密情報S1を用いて端末局1の公開情報Y_1が、

$$Y1=S1\cdot(G^{e1} \bmod n)$$

に従って定められる。このように中央局201は、図2に示すように、端末局1に関連する各種情報を作成すると共に、他の各端末局j，k，…に関連する情報をも作成する。

【0042】なお、中央201は更に各端末局1，j，…において時刻情報tに依存した情報であるいわゆるタイムスタンプTを作成するため疑似ランダム関数h_2（）を定める。次に、図1に示される暗号通信システムの端末局1，jの間での暗号通信方法を図3に示したフローチャートに従って説明する。なお、本実施例ではk＝2、すなわち$f=d^2$を用いている。

【0043】まずステップ301で、端末局1は中央局201から公開情報である法n、整数g，公開鍵e、疑似ランダム関数h_1（）及びh_2（）、公開情報Yj、及び数値IDj、並びに局秘密情報S1を入手する。

【0044】ステップ302では、鍵共有情報作成手段206において、乱数生成器204によって生成された乱数情報r_1及び時計205から得られる時刻情報t、並びに中央局201から入手した情報をもとにタイムスタンプT及び鍵共有情報X_{1j}が、

$$T=h_2(t)$$

$$X_{1j}=S1^{r1}\cdot(Yj^{r1}\cdot h_1(IDj))^{r1} \bmod n$$

に従って定められる。ステップ３０３では、送信側鍵生成手段２０７において共有鍵K_{ij}が、

$K_{ij}=g^{r_i} \bmod n$

に従って定められる。また同時にステップ３０４では、ステップ３０２で定められた鍵共有情報X_{ij}及び時刻情報ｔが端末局ｊへ送信される。

【００４５】ステップ３０５では、端末局ｊは中央局２０１から公開情報である法ｎ、公開鍵ｅ，疑似ランダム関数h_1（）及びh_2（）、及び数値ＩＤｊ、並びに局秘密情報d_jを入手する。

【００４６】ステップ３０６では、時刻妥当性確認手段３０８において時刻情報ｔの妥当性が確認される。本実施例では端末局ｊが処理を行っている現在時刻ｔ´と時刻情報ｔとの差が端末局ｉから端末局ｊへの伝送遅延程度であるか否かが確認される。すなわち適宜の許容誤差Δｔを用いて、

$t'-t<\Delta t$

であることを調べる。妥当性が確認された場合、ステップ３０７へ進み、妥当でない場合には第３者の成り済ましがあったものとして処理を中止する。

【００４７】ステップ３０７では、受信側鍵生成手段２１０において中央局２０１から入手した公開情報、局秘密情報、及び端末局ｉから送信された情報を基に、タイムスタンプT及び端末局ｊの共有鍵K_{ij}が、

$T=h_2(t)$

$K_{ij}=(X_{ij}^{e_j}\cdot h_1(IDi)^r)^{d_j} \bmod n$

に従って定められる。

【００４８】ステップ３０８では、端末局ｊは生成した共有鍵K_{ij}の値が、端末局ｉが生成した共有鍵K_{ij}の値に一致するか否かが暗号技術を利用して確認される。暗号通信によって端末局ｉと端末局ｊが同一の鍵情報を持つことを確認する具体的方法として以下の方法がある。

［プロトコル］

１．端末局ｉは乱数Ｒを生成し端末局ｉへ送る。

２．端末局ｊは別の乱数Ｒ´を生成し、共有鍵K_{ij}で乱数Ｒと乱数Ｒ´の連結を暗号化し、

$V=E(K_{ij}, R\|R')$

を得る。端末局ｊはＶを端末局ｉへ送る。

３．端末局ｉはＶを共有鍵K_{ij}で復号し、

$W=E(K_{ij}, V)$

を得る。Ｗの前半部が端末局ｉが最初に生成した乱数Ｒと一致していれば、端末局ｉは端末局ｊが共有鍵K_{ij}と同じ鍵を持っていることを確認する。また、端末局ｉはＷの後半部を端末局ｊへ送る。４．端末局ｊは端末局ｉから送られてきた情報が自分が生成した乱数Ｒ´に一致していれば端末局ｉが自局の鍵K_{ij}と同じ鍵を持っていることを確認する。

【００４９】この方法は秘密鍵暗号に基づく相手認証プロトコルと呼ばれる通信方法の一実現法である。相手認証プロトコルによれば、第３者に対して秘密にしたいK_{ij}又はK_{ji}を直接通信回線に流すことなしに相手局が自局と同じ鍵を所有していることを確認できる。なお、K_{ij}とK_{ji}が一致することを確認する方法はこの方法に限定されない。

【００５０】これが公開鍵の認証機能である。$K_{ij}=K_{ji}$であることが確認された場合、端末局ｊは正規の送信局から送信され、かつ伝送誤りのない暗号化された情報であると認証する。すなわち、端末局ｉ，ｊは同一の鍵を共有することになる。次に、第３者による成り済ましについて説明する。

【００５１】仮に、端末局ｊ以外の第３者が中央局２０１からＹｊなどの公開情報を得、更に何等かの方法で局秘密情報Ｓｉを盗用しても、従来と同様に第３者は乱数情報r_iの値を推定できなく、更に本実施例で用いている時刻情報ｔの値を知ることができない。それで、K_{ij}に暗号化された端末局ｉの送信電文の安全性は保たれることになる。

【００５２】また、第３者が端末局ｉに成り済まして端末局ｊに対し再送攻撃を行っても、その再送攻撃時の時刻情報t_0の値は端末局ｉの正規の送信時の時刻情報ｔと必ず異なることになるので、端末局ｊは再送攻撃に対し共有鍵K_{ij}の生成を中止する。次に、本実施例と岡本栄司氏の方式との違いを説明する。

【００５３】本実施例では共有鍵K_{ij}（$K_{ij}=g^{r_i} \bmod n$）は端末局ｉが定める乱数情報のみに依存し、端末局ｊに関するパラメータを含まない。このような特徴は３つ以上の端末局の間で鍵を共有する場合に大きな利点になる。すなわち、端末局ｉ，ｊ．ｋの三者が鍵共有する場合、端末局ｉは端末局ｊと上述の鍵共有方式を用いてK_{ij}を共有する。同様に端末局ｉは、同じ乱数情報及び時刻情報を用いて、同時に端末局ｋとK_{ik}を共有する。その結果、端末局ｉ，ｊ，ｋの三者間では$g^{r_i} \bmod n$を鍵として共有することになる。四者以上の場合でも全く同様である。

【００５４】なお、ここに示した鍵共有手続きには時刻情報ｔが含まれ、特定の時刻に作成された鍵共有情報X_{ij}は第３者による再送攻撃時には無効になるので、時刻情報ｔを利用した本発明は再送攻撃を防ぐことができる。

【００５５】しかしながら、この鍵共有法では、送信局ｉの秘密情報Ｓｉが、受信局ｊとｋの結託により漏洩する可能性がある。以下に受信局ｊとｋの結託による攻撃法を説明する。受信局ｊは、送信局ｉからの鍵配送情報X_{ij}と局秘密情報d_jから次のZ_{ij}を計算する。

$Z_{ij}=X_{ij}^{d_j} \bmod n=Si^{rd_j}\cdot G^{rr_j} \bmod n$

同様に、受信局ｋは、送信局からの鍵配送情報X_{ik}と局秘密情報d_kから次のZ_{ik}を計算する。

$Zik=X_{ik}^{d_k} \bmod n=Si^{rd_k}\cdot G^{rr_i} \bmod n$

受信局ｊとｋの結託により以下のＺｉを求める。

$Z_i=Z_{ij}/Z_{ik} \bmod n=Si^{r(d_j-d_k)} \bmod n$

13

【００５６】一方、$S1' = h_1(ID_i)^{-1} \bmod n$なる情報は公開されているのでGCD（e，T（$d_j - d_k$））＝1であれば、次式を満たす整数（a，b）をユークリッドの互除法により求められる。

$a \cdot e + b \cdot T(d_j - d_k) = 1$

この整数（a・b）を利用することにより、次式の計算でS1を求めることができる。

$(h_1(ID_i)^{-1})^{a} \cdot Z1^{b} = S1 \bmod n$

【００５７】以上の攻撃は、局秘密情報であるd_j，d_kを受信局が自由に利用できることを前提としている。逆に、局秘密情報d_j，d_kは受信局であってもその値を知らないデータであって、その秘密情報は鍵配送情報から鍵を求める段階の限られた用途にしか利用できないように装置構成されている状況では、上記攻撃は不可能である。

【００５８】以上のように、グループ鍵共有にも適用可能にするためには、特殊な装置構成を採用する必要がある。図４は、その一実施例である。図４に示した装置は、図３ステップ３０７におけるKij＝（$X_{ij}' \cdot h_1(ID_i)^{r})^{d_i} \bmod n$の計算を実行するものである。４０２，４０３，４０４の３つは、べき乗剰余計算器であり、４０５は剰余乗算器である。４０６は演算に必要な数値を格納するメモリであり、局秘密情報d_i、システムの公開鍵e、nが記憶される。４０１はこれらの要素部品を封止した媒体であり、例えばＩＣカードがこれに相当する。この装置の利用者は、（X_{ij}，$h_1(ID_i)$，$h_2(t)$）の３つのデータを入力として与えて、出力としてK_{ij}を得ることができる。しかし、利用者であってもメモリ４０６から局秘密情報d_iを読み出したり、あるいは、装置４０１内の信号の流れを変更したりすることはできない。図４には、べき乗剰余計算器３個と剰余乗算器１個を内蔵した装置を示したが、これらは、べき乗剰余計算器１個と剰余乗算器１個で構成することも可能であるし、ソフトウェアで実現することも可能である。また、装置４０１内に関数h_1，h_2の演算器を内蔵し、入力として（X_{ij}，ＩＤi，t）を与えるように構成することも可能である。さらには、暗証照合などの手法により正当な利用者であると判断した場合にのみ演算結果が得られるように構成することもできる。

【００５９】以上説明したように、本発明の方式では、送信側端末局ｉが乱数情報r_iを自ら生成するので、暗号通信の度に簡単に鍵共有情報X_{ij}及び共有する鍵k_{ij}を変えることができる。また、鍵共有のために通信ネットワークに流す鍵共有情報X_{ij}は時刻情報ｔに依存しているので、ある時刻に作成した鍵共有情報X_{ij}を後で再び利用することは困難である。さらに、鍵K_{ij}は送信者の乱数情報r_iのみに依存するので、多数の受信側端末局宛に個別に鍵共有情報を送ることで３者以上の間での鍵共有も可能である。実際に３者以上で安全に利用できるシステムとするためには、送信者秘密情報の漏洩を防止するために局秘密情報の不正使用が困難であるような装置構成を取る必要がある。

14

【００６０】さらには、本発明では、１つの素数を法とするのではなく２つの素数の積を法としているため、端末局認証用の局秘密情報を用いて認証機能を実現している。なお、３つ以上の素数の積を法とする方式に比べてメモリ、計算量の節約となる。次に、平文Mの暗号化及び解読のために適合された本発明の第２実施例に係わる暗号通信システムのブロック図を図５に示す。

【００６１】図示するように、本実施例の暗号通信システムは、第１実施例の暗号通信システムに送信側鍵生成手段２０７で生成される共有鍵K_{ij}を基に平文Mから暗号文Ｃを作成する暗号文生成手段２１２と、受信側鍵生成手段２１０で生成される共有鍵K_{ij}を基に暗号文Ｃを解読する復号手段２１３とを加えて構成される。

【００６２】上記構成において、図６に示したフローチャートに従い、送信側端末局ｉと受信側端末局ｊとの間で平文Mの暗号化及び解読をする暗号化通信方法について説明する。本実施例では前述した第１実施例と同様に、ｋ＝２とし、ステップ６０１では端末局ｉは中央局２０１から公開情報及び局秘密情報Ｓｉを入手する。

【００６３】ステップ６０２では、乱数情報r_i、時刻情報ｔ、公開情報、及び局秘密情報Ｓｉをもとに鍵共有情報作成手段２０６において、タイムスタンプT及び鍵共有情報X_{ij}が、

$T = h_2(t)$

$X_{ij} = Si' \cdot (Yj^{a} \cdot h_1(IDj))^{r} \bmod n$

に従って作成される。ステップ６０３では、ステップ６０２で定められた第１の暗号文C_1及び時刻情報ｔが端末局ｊへ送信される。また同時にステップ６０４では、端末局ｉは送信側鍵生成手段２０７において共有鍵K_{ij}が、

$K_{ij} = g^{r} \bmod n$

に従って定められる。ステップ６０５では、暗号文生成手段２１２において平文Mが上記共有鍵K_{ij}を用いて、

$C = E(K_{ij}, M)$

に従って暗号文Ｃに暗号化される。ここで、記号Ｅ（K_{ij}，Ｍ）は共有鍵K_{ij}に基づいて平文Mを暗号化する手続を表す。代表例として、ＤＥＳ方式及びＦＥＡＬ方式が挙げられる。

【００６４】次いで、端末局ｊはステップ６０６において中央局２０１から公開情報である法ｎ、公開鍵ｅ、非負整数ｋ、疑似ランダム関数h_1（ ）及びh_2（ ）、及び数値ＩＤｊ、並びに局秘密情報d_iを入手する。

【００６５】次いで、ステップ６０７では時刻妥当性確認手段２０８において時刻情報ｔの妥当性が確認される。この確認手順は第１実施例と同様である。妥当性が確認された場合、ステップ６０８へ進み、妥当でない場合には第３者の成り済ましがあったものとして処理を中

止する。

【0066】ステップ608では、受信側鍵生成手段210において中央局201から入手した公開情報、局秘密情報d_i、及び端末局iから送信された鍵共有情報X_{ij}及び時刻情報tを基に、タイムスタンプT及び端末局jの共有鍵K_{ij}が、

$T=h_3(t)$

$K_{ij}=(X_{ij}^{e}\cdot h_1(ID\,i)^{r})^{d_j} \bmod n$

に従って定められる。ステップ609では、復号手段213において暗号文Cが上記共有鍵K_{ij}を用いて以下のように復号される。

$M'=D(K_{ij}, C)$

【0067】ここで、記号$D(K_{ij}, C)$は暗号文Cを共有鍵K_{ij}で復号する手続を表す。次にステップ610において、端末局jは復号されたM′の内容を確認する。もし復号文M′が意味のある内容であるならば暗号文Cは送信局側で正しい鍵で暗号化され、通信途上でも誤り又は改ざんが生じなかったことが確認できる。不正な第3者が成り済ましを試みても、正しい鍵を知らないのでここで不正が発覚する。なお、復号文M′が正しく復号された意味のあるメッセージかどうかを受信側で自動的に確認したい場合には、予め送受信者間で取り決めた冗長性をメッセージMに付加しておけば良い。

【0068】なお、ステップ610での確証機能が必ずしも必要でない場合には、k＝0、S i＝S j＝1、及び$h_1(ID\,i)=h_1(ID\,j)=1$と設定しても良い。従って、平文Mは暗号文生成手段212で暗号化された後に受信側端末局jへ送られ、該受信側端末局jの復号手段213において時刻情報tに依存した鍵共有情報X_{ij}を用いて解読されるので、第1の実施例と同様に、成り済ましによるメッセージの再送攻撃を受ける恐れがない。

【0069】次に、上記第2実施例を利用して暗号化された電子メールを送受信する第3実施例に係わる暗号通信方法及び暗号通信システムについて図7乃至図11を用いて説明する。本実施例においても従来例で説明した同報通信機能及び受信者不在を通知する機能がサポートされており、図7に暗号通信システムの概念図を示す。

【0070】図示するように、ユーザ1乃至ユーザ5が双方向通信の伝送路6、7、8、9及び10で接続される。ここで、ユーザ1乃至ユーザ5のそれぞれは第2実施例における各端末局に対応する。

【0071】また、ユーザ1からユーザ2を介してユーザ4へ送信され宛先不明のため返信されたメールの伝送経路11と、ユーザ1からユーザ3へ送信されたメールの伝送経路12とが破線で示されている。

【0072】ユーザ1乃至ユーザ5のそれぞれは第2実施例におけける各端末局と同様に中央局201に通信ネットワークを介して接続され、中央局201から公開情報及び局秘密情報を入手する。図8にユーザ1において

メールを暗号化し、次いでユーザ3において暗号化されたメールを復号する暗号通信システムの一部のブロック図を示す。

【0073】図示するように、本実施例に係わる暗号通信システムは第2実施例の暗号通信システムの第1暗号文生成手段211を鍵共有情報作成手段206に置き換え、更に送信部202に送信電文作成部214と、受信部203に受信電文分離部215とを追加して構成される。

【0074】送信電文作成部214は鍵共有情報作成手段206で作成される鍵共有情報X_{ij}、暗号文生成手段212で生成される暗号文C＝E（K, M）、時計205から出力される時刻情報t，及び中央局201からの番号ID i（i＝1、2、…）を基にして図9に示されるビット列から成る送信電文（電子メール）を作成する。

【0075】受信電文分離部215は送信電文作成部214から送信される電文を受信し、該電文から自局に係わる鍵共有情報X_{ij}及び番号ID iを受信側鍵生成手段210へ、時刻情報tを時刻妥当性確認手段208へ、第2暗号文C＝E（K, M）を復号手段213へ送る。ここで、暗号文C＝E（K, M）はユーザiからユーザjへ送信される同報通信の平文Mの暗号文を意味する。

【0076】なお、図7に示す電文の送信の場合には、送信電文は、図10に示すように送信者のアドレスID_1；受信者のアドレスID_3，ID_4、鍵共有情報X_{11}、X_{13}，X_{14}、時刻情報t、及び暗号文C＝E（K, M）から構成される。但し、Kは乱数r_1から送信側鍵生成手段207で作成される鍵情報である。ユーザ1、3、4における受信側鍵生成が正しく行われた場合には、$K=K_{11}=K_{31}=K_{41}$が成り立つ。

【0077】以上の構成において、ユーザ1の送信電文作成部214で作成された電文は伝送経路12を通ってユーザ3へ送信され、ユーザ3の受信電文分離部215において送信者のアドレスID_1、鍵共有情報X_{13}、時刻情報t、及び暗号文C＝E（K, M）が選び出される。これらの情報を基にして、第2実施例と同様に暗号文C＝E（K, M）が復号されて平文Mが得られる。ユーザ3がこの暗号文を復号できる理由は$K=K_{31}$となるからである。また、同様にユーザ1からユーザ4へも同時に電文が送信される。

【0078】ここで、例えばユーザ4の宛先が不明で電文がユーザ1に返送されてきた場合、ユーザ1は鍵共有情報X_{11}を選び出し、次いで受信者と同様に暗号文C＝E（K, M）を復号するための共有鍵K_{11}を作成する。なすわち、

$T=h_3(ID_1)$

$K_{11}=(X_{11}^{e}\cdot h_1(ID_1)^{r})^{d_1} \bmod n$

ユーザ1は上記手順で作成した鍵K_{11}を用いてC＝E（K, M）を復号する。すなわち、上記共有鍵K_{11}を用

いて暗号文C＝E（K，M）が、
M´＝D（K_{11}，C）
に従って復号文M´に復号される。この復号文M´は平文Mに一致する。

【００７９】従って、本実施例の暗号通信システムを用いることにより、一のユーザから多数の他のユーザへ暗号化された電子メールを同時に送信することが可能である。もちろん宛先となっているユーザ以外のユーザから盗聴される虞は無い。また、鍵共有情報X_{11}は乱数情報r_1及び時刻情報tから作成されるので、第３者の成り済ましによる再送攻撃を受ける虞がない。また、電子メールを受信するユーザは自局に関係する情報のみを取り出し、暗号化された電子メールを復号することができる。

【００８０】さらに、図１１に示すように宛先不明のためメッセージが送信側のユーザに返送されても、共有鍵X_{11}を送信文に付加しているため、送信者側のユーザは暗号化された電子メールを容易に復号できる。つまり、いかなる内容のメッセージが相手に届かなかったのかを確認することができる。

【００８１】上記実施例では、各ユーザの間は全て双方向の伝送路で網目状に接続しても良い。また、選択次第では、電子メールの伝送は他のユーザを介して行えるので、使用状況に応じて必要最小限の伝送路のみを用いても良い。また、本実施例では多数のユーザに電子メールを同時に伝送したが、受信側のユーザが単一であっても良い。

【００８２】また、図９に示した送信電文には、更に付加的な情報として、例えば伝送誤りを訂正するためのパリティビットなどを付け加えても良い。また、送信電文内の配列順は適宜変えても良い。

【００８３】次に、上記第２実施例を利用して暗号化されたデータをファイルに格納する第４実施例に係わる暗号通信方法及び暗号通信システムについて図１２乃至図１６を用いて説明する。

【００８４】本実施例は、計算機で扱うデータのセキュリティを確保するための一方法として、ファイル毎にユーザがデータの内容を暗号化して適宜のメモリに格納し、必要に応じて上記データ内容を復号して用いる方法を具現化したものである。

【００８５】本実施例の暗号通信システムの端末局の構成は第３実施例と全く同様であるが暗号化されたデータの行き先が異なる。つまり、図１２に本実施例と第３実施例を比較して示すように、第３実施例では作成された暗号情報はメッセージとして伝送路を介して相手のユーザへ送られたが、本実施例では作成された暗号情報は送信部２０２から記憶装置にファイルとして格納され、別の時刻に受信部２０３を介して読み出される。

【００８６】図１３にユーザ１がデータMを暗号化してメモリに格納し、必要になったときにメモリから読み出し復号する場合の概念図を示す。この場合のメモリに格納されるファイルの構成は図１４に示される。すなわち、ファイルはフィイルヘッダにファイルＩＤ、ユーザＩＤ、鍵復元情報X_{11}、時刻情報tを有し、ファイル本体に暗号化データC＝E（K，M）を有する。ここで、暗号鍵Kは、

$K = g^{r_1} \bmod n$

によって定まり、鍵復元情報X_{11}は第３実施例と同様に定まる。復元する場合も第３実施例と同様に復元鍵K_{11}が生成される。つまり、このとき正しく鍵が復元されれば$K = K_{11}$が成り立つ。

【００８７】図１５に読み出し可能なユーザを複数に拡張した場合の概念図を示す。つまり、ユーザ１のみならず、ユーザ３、ユーザ４も同様に読み出すことが可能である。この場合のメモリに格納されるファイルの構成は図１６に示される。すなわち、ファイルはファイルヘッダにファイルＩＤ、ファイル作成者ID_1、ファイル利用者ID_1、ID_3、ID_4、鍵復元情報X_{11}、時刻情報tを有し、ファイル本体に暗号化データC＝E（K，M）を有する。

【００８８】図１６ではファイル作成者ID_1とファイル利用者ID_1が重複するのでファイル利用者ＩＤ記入フィールドのID_1は省略されている。ID_1をこのフィールドに陽に書いておいても良い。従って、本実施例の暗号通信システムはファイルを暗号化してメモリすると共に、必要に応じて読み出し復元する暗号通信方法に適用可能である。本発明は、上記実施例に限定されるものではなく、適宜の設計的変更により、適宜の態様で実施し得るものである。

【００８９】

【発明の効果】以上説明したように本発明の暗号通信方法によれば、前記中央局が全ての端末局に公開する同一の公開情報及び各端末局のそれぞれに知らせる相異なる局秘密情報を作成する工程と、前記中央局が前記公開情報及び前記局秘密情報を暗号送信側の端末局及び暗号受信側の端末局に発行する工程と、前記送信側端末局内で乱数情報を生成する工程と、前記送信側端末局内で時刻情報を出力する工程と、前記乱数情報及び前記公開情報に基づき送信側の鍵を生成する工程と、前記乱数情報、前記時刻情報、前記公開情報及び前記局秘密情報に基づき鍵共有情報を作成する工程と、前記時刻情報及び前記鍵共有情報を受信する端末局内で前記時刻情報が虚偽であるか否かを確認する工程と、前記受信側端末局内で前記時刻情報が虚偽でないと確認された場合、前記時刻情報、並びに前記鍵共有情報、前記公開情報及び前記局秘密情報に基づき受信側の鍵を生成する工程と、前記送信側端末局内で生成された鍵と前記受信側端末局内で生成された鍵とが一致することを両者の比較により確認して一致した場合に正規の暗号であると認証する工程とを備えたので、共有する鍵の変更が容易であり、３者以上の

19

間での鍵共有も可能であり、かつ成り済ましによる再送攻撃を有効に防止することが可能である。

【００９０】また、本発明の暗号通信システムは上記暗号通信方法におけるそれぞれの工程に対し対応する手段を設けたので、上記暗号通信方法を実施するに有用である。選択次第では、鍵共有情報を作成する工程で作成される鍵共有情報には送信側端末局自身で前記暗号化された平文を復号する宛先不明用鍵共有情報が含まれ、送信側鍵生成手段で生成された送信側の鍵を用いて平文を暗号化する平文暗号化手段と、該手段で暗号化された前記平文、並びに前記鍵共有情報作成手段で作成される鍵共有情報及び時刻情報出力手段で出力された時刻情報から送信電文を作成する送信電文作成手段と、該手段で作成された電文を受信側端末局で受信し電文内容を分割する電文内容分割手段と、該手段で分割された前記暗号化された平文を受信側鍵生成手段で生成された受信側の鍵を用いて復号する復号手段とを備え、更に受信側端末局の宛先が不明の場合、前記宛先不明用鍵共有情報に基づいて送信側端末局自身が前記暗号化された平文を復号する送信側復号手段を有したので、電子メールの送受信において宛先に電子メールの受信者が存在しない場合でも通信システムを複雑にすることなく対処可能である。

【図面の簡単な説明】

【図１】　本発明の第１の実施例に係わる暗号通信システムのブロック図。

【図２】　中央局及び端末局で作成される情報の説明図。

【図３】　図１に示した暗号通信システムの端末局間での暗号通信方法を説明するフローチャート図。

【図４】　３者以上の鍵共有を行う暗号システムに利用される演算装置の構成図。

【図５】　本発明の第２の実施例に係わる暗号通信システムのブロック図。

【図６】　図５に示した暗号通信システムの暗号通信方法を説明するためのフローチャート図。

【図７】　本発明の第３の実施例に係わる暗号通信方法の概念図。

20

【図８】　図７に示した暗号通信方法を実現する暗号通信システムのブロック図。

【図９】　図８に示した暗号通信システムで作成された送信電文図。

【図１０】　ユーザ１からユーザ３及びユーザ４へ送信される電文図。

【図１１】　宛先不明のためメッセージが送信側のユーザに返信された場合の処理の説明図。

【図１２】　本発明の第４と第３の実施例との比較図。

【図１３】　図に１２に示した暗号通信方法を説明するための概念図。

【図１４】　図に示したメモリに格納されるフィルタの構成図。

【図１５】　図１２に示した暗号通信方法に対し読み出し可能なユーザを複数に拡張した場合の概念図。

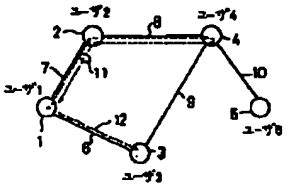
【図１６】　図１５に示したメモリに格納されるファイルの構成図。

【図１７】　従来例を示した図。

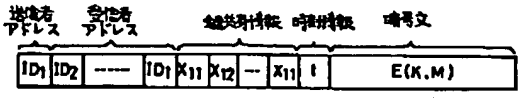
【符号の説明】

２０１…中央局,
２０２…送信部,
２０３…受信部,
２０４…乱数生成器,
２０５…時計,
２０６…鍵共有情報作成手段,
２０７…送信側鍵生成手段,
２０８…時刻妥当性確認手段,
２０９…秘密鍵メモリ,
２１０…受信側鍵生成手段,
２１２…暗号文生成手段
２１３…復号手段,
２１４…送信電文作成部,
２１５…送信電文分離部,
４０１…演算装置,
４０２、４０３、４０４…べき乗剰余計算器,
４０５…剰余乗算器,
４０６…データ・メモリ。

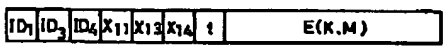
【図７】



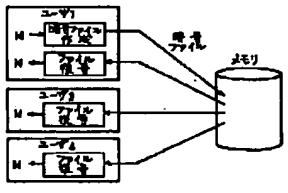
【図９】



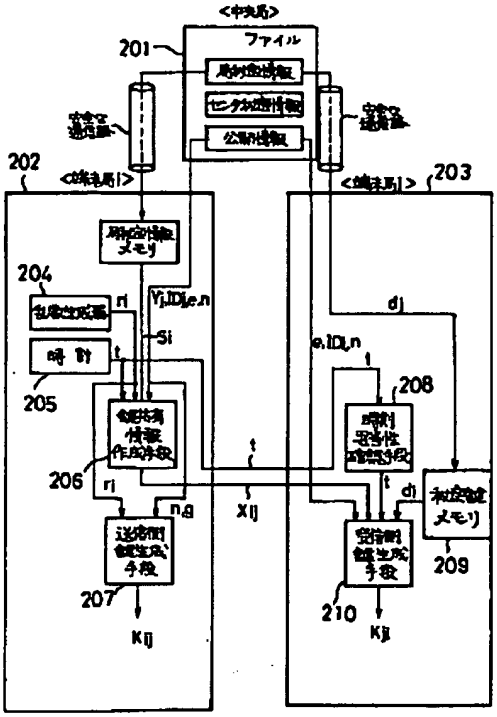
【図１０】



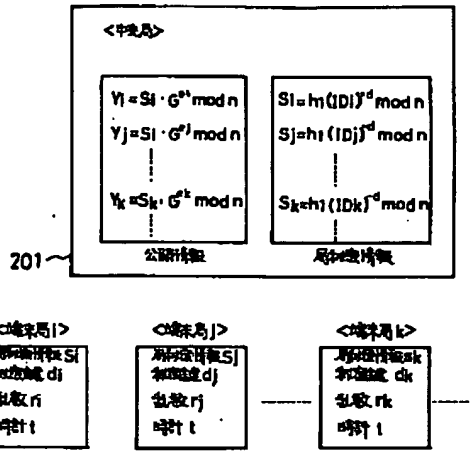
【図１５】



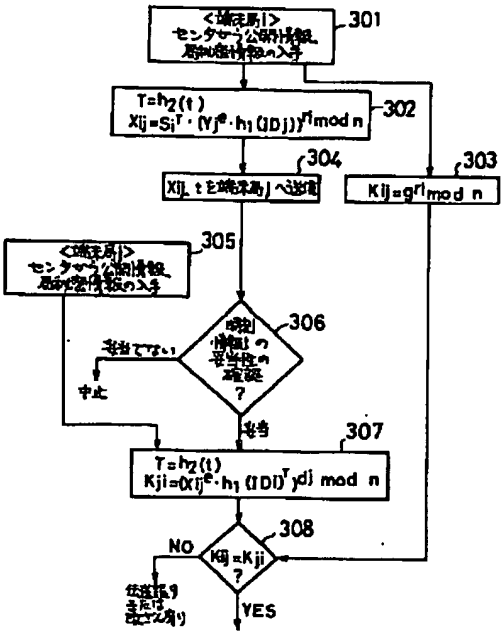
【図1】



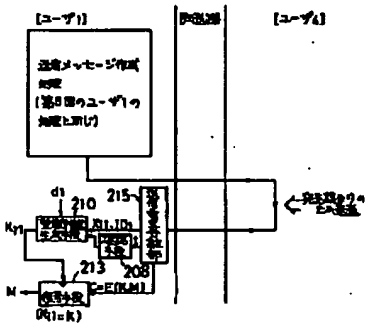
【図2】



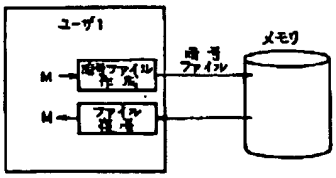
【図3】



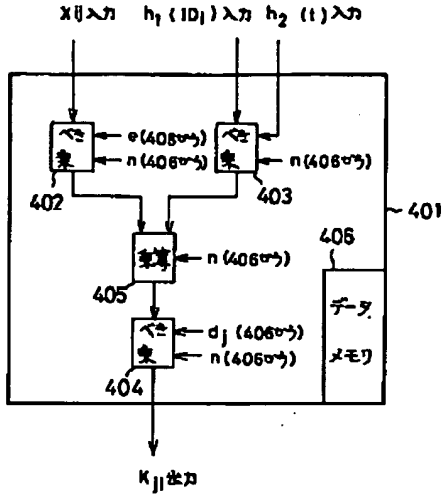
【図11】



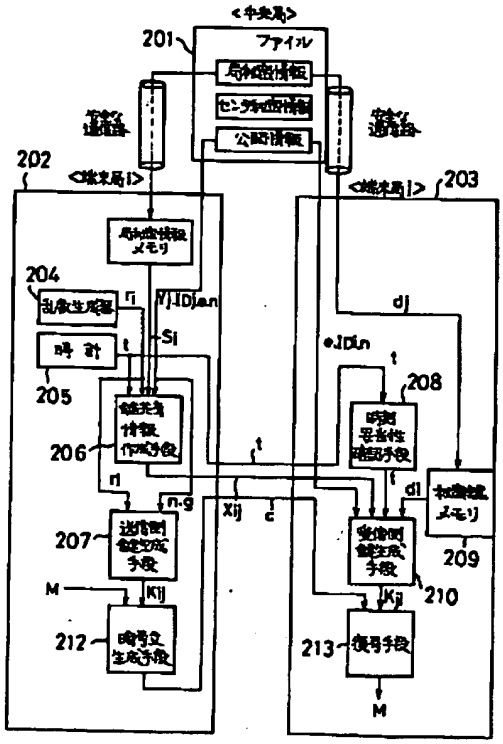
【図13】



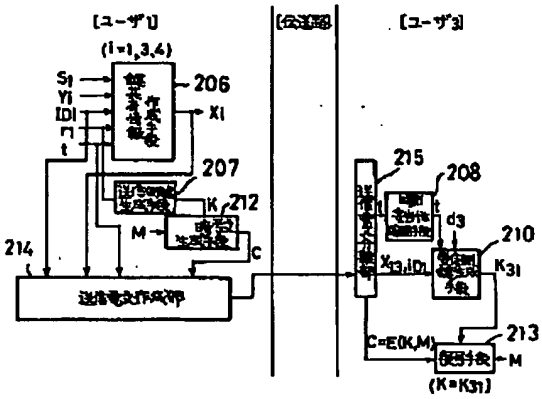
【図4】



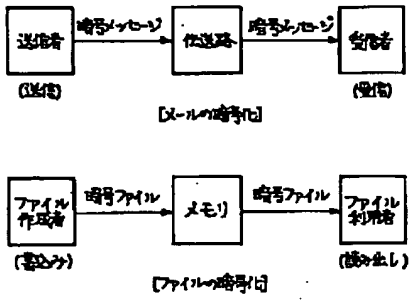
【図5】



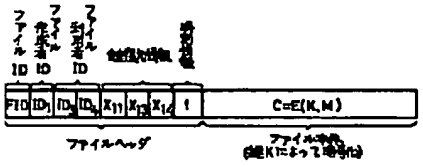
【図8】



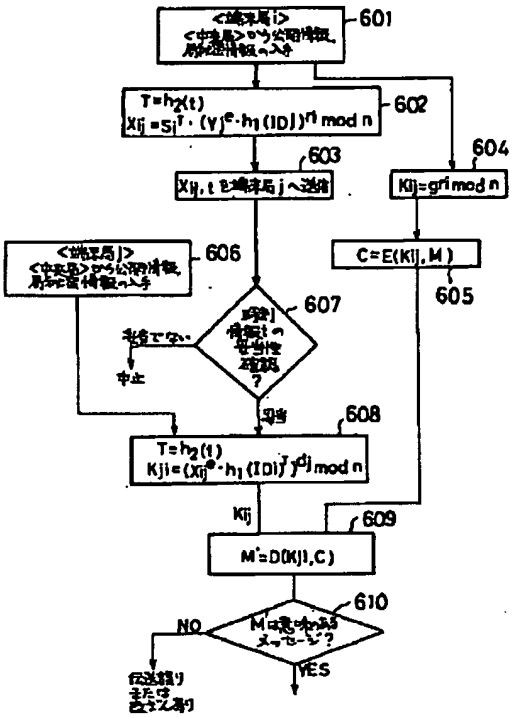
【図12】



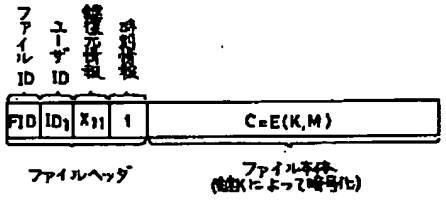
【図16】



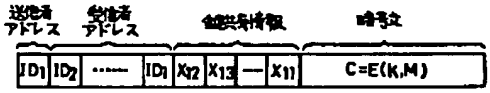
【図6】



【図14】



【図17】



フロントページの続き

(51)Int.Cl.⁵	識別記号	庁内整理番号	F I	技術表示箇所
H04L 12/54				
12/58				